



Atoms for Peace

الوكالة الدولية للطاقة الذرية

國際原子能機構

International Atomic Energy Agency

Agence internationale de l'énergie atomique

Международное агентство по атомной энергии

Organismo Internacional de Energia Atómica

Ms. Barbara Hoffheins

ISPO Liaison Officer

U.S. Mission to the International Organizations in
Vienna (UNVIE)

Wagramer Strasse 17-19

A-1220 Vienna

Austria

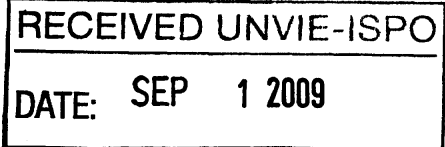
Wagramer Strasse 5, PO Box 100, 1400 Wien, Austria

Phone: (+43 1) 2600 • Fax: (+43 1) 26007

Email: Official.Mail@iaea.org • Internet: <http://www.iaea.org>

In reply please refer to: M2.05-USA

Dial directly to extension: (+431) 2600-21814



2009-08-31

Dear Ms. Hoffheins,

With reference to the US Support Programme, I am pleased to provide the attached new cost-free expert task proposal with a copy of the relevant job description for your consideration.

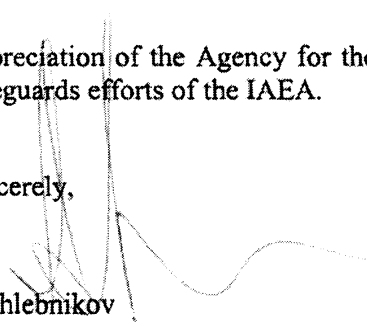
The Department of Safeguards would appreciate the nomination of more than one candidate. This will allow the Department to perform an evaluation of candidates that will result in the most suitable candidate being selected for the task. So that this process may proceed on a timely basis, I have listed the proposal below along with a closing date for nominations and expected start date. Also in order to facilitate the selection process, I would like to ask you to send the candidates' Curricula Vitae and an Agency Personal History Form with the nomination. Of course all information will be treated as confidential.

SP-1 Number	Title	Expected Start Date	Closing Date f. Nominations
09/ICO-002	Expert – Monitoring and Availability Engineer	As soon as possible	As soon as possible

I will inform you of the result of the evaluation as soon as a decision is made. The final documentation for the successful candidate can then be completed through the Support Programmes Coordination and the Division of Human Resources.

I would also like to take this opportunity to express the appreciation of the Agency for the valuable contribution provided by your Support Programme to the safeguards efforts of the IAEA.

Yours sincerely,



Nikolai Khlebnikov
Director
Division of Technical Support
Department of Safeguards

Enclosure

SP-1 TASK PROPOSAL PART

1. Task Proposal

- 1.1 Task Proposal ID: 09/ICO-002 Date received in SPA: 2009-02-25
- 1.2 Task Title: Expert - Monitoring and Availability Engineer
- 1.3 Requester / Division / Section: Pichan / SGIM / ICO
- 1.4 Is this a CFE task? Yes
- 1.5 Task Category: X
- 1.6 Is this a joint task for MSSPs? No
- 1.7 Is multiple acceptance required? No

If 1.6 or 1.7 is yes, indicate the reason:

2. Project

- 2.1 Project ID: SGIM-001 Project Type:
- 2.2 Project Title: Integrated Safeguards Environment
- 2.3 Project Manager / Division / Section: Kirkgoetze / SGIM / IAP

3. Safeguards Requirement Identification

3.1 What is needed, why and when:

The Integrated Safeguards Environments (ISE) is the new computing environment upon which Safeguards business will be run in the coming decade and beyond. A Service Oriented Architecture (SOA) has been adopted and the necessity to provide 24/7 IT services to the department of Safeguards is paramount. In order to achieve this goal, proactive monitoring of hardware and software is required. ICO has taken the first step of this goal by installing and performing basic configuration of a monitoring infrastructure. However, an IT expert who is skilled and experienced with the monitoring of Microsoft operating systems, server applications, and component applications is needed to further configure and exploit the monitoring infrastructure established by ICO, with the intent of delivering a service-level and business-level view to both IT and Safeguards Business users. An end-to-end service management capability is the key driver for this project.

3.2 How will the task results be used and by whom:

The resulting enhanced monitoring will result in higher IT service availability. Detailed and proactive monitoring will provide system engineers with the information required to tune and optimize operating systems and server applications. Application developers and SG's application development partners will utilize the infrastructure and tools to produce custom management capabilities for each application introduced into the environment. IT leaders will be able to view the availability and performance of IT services provided in real time or utilized the output of this project to conduct impact analysis, capacity planning and historical reporting. Business users will be able to view a dashboard of business processes supported by IT.

3.3 Consequences if task is not performed:

Without support of an expert in this area, ICO is exposed to a risk of compromised availability of mission critical IT services. The ability to effectively monitor the ISE infrastructure at the service level is crucial for successful IT service delivery to Safeguards users.

4. IAEA Proposed Work Outline

4.1 Major task stages with timing:

- Analysis and detailed requirement gathering of monitoring needs of ISE. This will include close work with application developers, system engineers, system end-users and service desk personnel (3 months).
- Implementation of an ITIL-compliant monitoring system which interfaces with the ITIL processes for incident, change and problem management capabilities already extant in SGIM or improved versions provided by the expert. Alert the proper individuals at the proper level for all phases of service management. Assist with the design and development of a system for Services Oriented Architecture runtime governance including managing service capacity, performance, availability as well as trend and impact analysis. Design and develop the end user interfaces for the service availability tools (18 months).
- Thorough documentation of approach, design and implementation of service definitions and service relationships must be created. Technical documentation will include the descriptions of all custom written scripts, relationships among various software components used, security features and operational issues and instructions (3 months).

Work plan outline:

March 2010 - Analysis and requirements gathering

October 2010 - Solution design and Implementation

Sept 2011 - Follow up actions, documentation

4.2 Support Division(s) / Section(s): SGIM / IAP, ICO

4.3 End User Division(s) / Section(s): SGIM / IAP, ICO

4.4 Estimated duration in months: 24

5. Safeguards Approval Process - not displayed

6. Acceptance by MSSP(s)

6.1 MSSP(s) to which the task is proposed:

USA

Date accepted:

Agency Task ID:



Job Description for Professional Posts

Position and Grade:	Monitoring and Availability Engineer ([P-3])
Organizational Unit:	Customer Services and Operations Section Division of Information Management Department of Safeguards
Duty Station:	Vienna, Austria
Type/Duration of Appointment:	2 Year Cost Free Expert (09/ICO-002)

Organizational Setting

The Department of Safeguards is the organizational hub for the implementation of IAEA safeguards. The IAEA implements nuclear verification activities for more than 160 States in accordance with their safeguards agreements. The safeguards activities are undertaken within a dynamic and technically challenging environment including advanced nuclear fuel cycle facilities and complemented by the political diversity of the countries.

The Division of Information Management comprises four sections and provides the Department of Safeguards with the services relating to data processing, secure information distribution, information analysis and knowledge generation necessary to draw independent, impartial and credible safeguards conclusions.

The Customer Services and Operations Section provides 24/7 quality computer services to the Department of Safeguards, and is run in compliance with best practices defined by international standards, in particular ITIL and ISO 17799, while the development of the infrastructure and database landscape follows best practices project management, in close coordination with the Information Architecture and Projects Section. The Customer Services and Operations Section, which operates in an environment where protection of confidential information is paramount, comprises four units: Network Operations; Customer Services; Data Integration; Support and Coordination.

The Network Operations Unit manages the infrastructure required for secure data communication within the Department and for secure external connections to facilities, IAEA Regional Offices, inspectors in the field and Member States; manages the infrastructure required for secure safeguards applications; provides ICT security services; and is responsible for electronic role-based access authentication services to ensure the proper availability, integrity, and confidentiality of safeguards information.

Main Purpose

Under the general supervision of the Head of the Network and Operations Unit, the Monitoring and Availability Engineer is responsible for monitoring of network and server hardware, Windows operating systems and applications, collection and consolidation of heterogeneous system log files, and to ensure the smooth operation of the backup and restoration infrastructure.

Role

The Monitoring and Availability Engineer performs the role of network administrator performing network design, configuration and management, system availability management performing the backup infrastructure management and project team leader.

Partnerships

The Monitoring and Availability Engineer works closely with other members in the Division of Information Management to provide monitoring, implement projects and solve problems. The Monitoring and Availability Engineer will, in particular, be working closely with members of the database team, application development Section, server administration team, and web server team to provide monitoring for availability and performance.

Functions / Key Results Expected

- Support: Manage the entirety of the Safeguards network and server monitoring and backup infrastructure, including planning and deployment of systems and software, daily operations, event monitoring and to ensure consistent and accurate monitoring of the systems. The infrastructure includes networking equipment such as switches, firewalls, Intrusion Prevention and Detection Systems, VPN devices and a Wide Area Network, conventional and blade servers, Storage Area Networks (SANs), fibre channel networks, Windows operating systems, database systems, e-mail systems, web servers, file servers, etc., located at multiple sites worldwide. Manage the backup infrastructure to ensure that all data resources are protected against data loss. Design and implement a business continuity and disaster recovery plan.
- System Centre Operations Manager (SCOM) configuration and management. Ensure the Systems/Services availability, detect and solve any service issues pro-actively.
- Problem investigation and solution: Participate in incident detection and resolution
- Security: Assist with the design and implementation of technical security solutions for the Department and, working with the entire Agency; Assist IT Vulnerability Experts with event log consolidation and management.
- Maintenance: Ensures continuous monitoring of the availability, and performance of IT services (software, hardware and operating systems).

Knowledge, Skills and Abilities

- Excellent knowledge of and experience with Microsoft System Center Operations Manager and Microsoft Windows Server Operating System. (Windows 2003/2008)
- Very good knowledge of Microsoft based server applications such as SQL Server, Windows Internet Information Server, Sharepoint server, ISA, Microsoft Exchange, BizTalk Server, ISA. Must have the ability to communicate and coordinate with area experts to provide appropriate and customized monitoring solutions.

- Good knowledge and demonstrated experience with NetBackup and Backup Exec backup software and enterprise level backup procedures.
- The ability to both take direction and work independently within an ITIL-informed environment, while handling multiple simultaneous operational and project duties.
- Strong interpersonal skills, the ability to self-manage, as well as analytical, effective communication, team leadership and strategic management skills.
- Excellent verbal and writing skills
- Excellent problem solving skills
- Knowledge of ITIL processes and Prince2 desirable

Education, Experience and Language Skills

- University degree in computer science, information technology or related technical discipline
- At least seven years total experience with Microsoft Windows operating systems
- At least five years experience with Microsoft Windows monitoring software
- At least three years experience with enterprise level backup software
- Experience with Microsoft System Center Configuration Manager, PowerShell, HP Insight Manager and knowledge of .net application development are pluses.
- Experience in an SOA environment is a definite advantage. Experience with business continuity and disaster recovery projects a definite plus
- Prior experience with ArcServe backup software would be beneficial
- Fluency in written and spoken English

Internal Human Resources use only:	
Effective Date:	
Occupational Group(s):	
Post Number:	